WHAT IS CLAIMED IS:

1. A method for providing scalable security services, comprising:

instantiating at least one application on the computer system; and

instantiating a Key Repository process on the computer system, the Key Repository process configured to

manage sensitive information in a database on the computer system using at least one master key,

validate and record authorizations of specific applications to access sensitive information in the database, wherein each of the at least one application is configured to query the Key Repository process for some or all of the sensitive information in the database, and

in response to the query from a particular instance of the at least one application, provide to the particular instance of the at least one application the requested some or all of the sensitive information only if the Key Repository process authenticates the particular instance of the at least one application as being pre-authorized to receive the requested some or all of the sensitive information.

2. The method of claim 1, wherein the at least one master key is divided into a predetermined number of portions each of which associated with a password, and wherein the sensitive information cannot be exposed without at least some or all of the predetermined number of passwords using a password-based private key encryption-decryption.

3. The method of claim 1, wherein the Key Repository process is a centralized repository process for the at least one master key, as well as passwords, enterprise policy and policy decisions, authorizations to use enterprise credentials and pre-authorization and authentication of the at least one application.

4. The method of claim 1, wherein the at least one master key is configured as an encryption key that maintains the integrity of and protects the sensitive information.

5. A cryptographic system in a computer system, the cryptographic system comprising:

at least one server;

a database, the database configured to contain sensitive information, the database responsive to signals from one of the at least one server;

at least one application on one of the at least one server; and

a Key Repository process on one of the at least one server, the Key Repository process using at least one master key for managing the sensitive information in the database, the Key Repository process further configured to validate and record authorizations to access sensitive information in the database, the at least one application configured to query the Key Repository process for some or all sensitive information in the database, and, in response to the query from a particular instance of the at least one application, the Key Repository process further configured to provide the requested some or all of the sensitive information to the particular instance of the at least one application but only if the Key Repository process authenticates the particular instance of the at least one application as being pre-authorized to receive the requested some or all of the sensitive information.

6. A cryptographic system as in claim 5, wherein the at least one master key maintains the integrity of and protects the sensitive information in the database.

7. A cryptographic system as in claim 5, wherein the at least one master key provides privacy protection to the sensitive information on the database.

8. A cryptographic system as in claim 5, wherein the sensitive information is a public key.

9. A cryptographic system as in claim 5, wherein the sensitive information is a secret.

10. A cryptographic system as in claim 5, wherein the sensitive information is a private key.

11. A cryptographic system as in claim 5, wherein the sensitive information is a symmetric key.

12. A cryptographic system as in claim 5, wherein the sensitive information is a certification authority certificate.

13. A cryptographic system as in claim 5, wherein each of the at least one master key are kept in physical memory.

14. A cryptographic system as in claim 5, wherein each of the at least one master key are kept in non-swappable physical memory.

15. A cryptographic system as in claim 14, wherein the non-swappable physical memory is protected.

16. A cryptographic system as in claim 5, wherein each of the at least one master key are kept in virtual memory.

17. A cryptographic system as in claim 5, wherein the at least one master key includes an integrity key configured to ensure the integrity of the sensitive information on the database.

18. A cryptographic system as in claim 5, wherein the at least one master key includes a protection key configured to protect the sensitive information on the database.

19. A cryptographic system as in claim 5, wherein the at least one application is a context-free server program.

20. A cryptographic system as in claim 19, wherein the at least one application is configured to retain context information across one or more instantiations of the at least one application.

21. A cryptographic system as in claim 20, wherein the context information includes sensitive data.

22. A cryptographic system as in claim 19, wherein the at least one application is configured to convey sensitive context information, by encrypting the information and then passing the information to a next instance of the at least one application.

23. A cryptographic system as in claim 9, wherein the secret is divided among a plurality of individuals.

25. A cryptographic system as in claim 23, wherein the integrity of the secret that is controlled by a first individual is increased by linking the secret to a second secret, the second secret is revealed only with the cooperation of all or a predetermined number of the plurality of individuals.

25. A cryptographic system as in claim 9, wherein the secret is protected by a password.

26. A cryptographic system as in claim 25, wherein the secret can be updated in the absence of the password.

27. A method for obtaining cryptographic credentials by an application running on a computer system, the method comprising the steps of:

(a) providing a computer system having at least one server;

(b) instantiating a Key Repository process on the computer system, the Key Repository process having a cryptographically protected database;

(c) instantiating an application process on behalf of an end entity on the computer system, the end entity having credentials stored in the database;

(d) requesting the Key Repository process for the credentials of the end entity by the application process; and

(e) if the Key Repository process authenticates the application process as having been pre-authorized to have the credentials, building an encrypted credentials file and providing the application process with the file and a password for the file.

28. A method as in claim 27, the method further comprising the steps of:

(e) instantiating a remote Key Repository process on a remote server.

29. A method as in claim 27, the method further comprising the step of:

(e) instantiating a local agent on a remote server.

30. A method as in claim 28, the method further comprising the step of:

(f) providing the Key Repository process with a remote agent interface; and

(g) linking the remote Key Repository process on the remote server to the Key Repository process via the remote agent interface.

31. A method as in claim 29, the method further comprising the step of:

(f) providing the Key Repository process with an agent interface; and

(g) linking the local agent on the remote server to the Key Repository process via the agent interface.